

What is claimed is:

1. A method for issuing a certificate using biometric information in a public key infrastructure-based authentication system including a registration authority, a
5 certificate authority and a user system, the method comprising the steps of:

a) receiving a certificate issuance request message containing a user's reference number and biometric information
10 sent from the user system under the condition that a user accesses the authentication system using the user system via the Internet to request a certificate issuance;

b) extracting the user's reference number and biometric information from the certificate issuance request message to
15 authenticate the user in connection with the certificate issuance request;

c) determining whether the biometric information is the same as user's biometric information stored in a database storage unit in such a way as to be matched with the reference
20 number under the condition that the user is registered as a member in the authentication system;

d) generating an authentication code of the user having requested the certificate issuance and providing the generated

authentication code to the user system; and

e) receiving a public key from the user system and issuing the certificate if the user system generates the public key.

5

2. The method of claim 1, wherein the step d) includes the steps of:

10 d1) receiving the authentication code from the authentication system and generating a private key and a public key; and

d2) sending the generated public key to a server of the certificate authority to be issued the certificate.

15 3. The method of claim 1, wherein the step e) includes the steps of:

20 e1) if receiving the public key at the step e), determining using the public key whether the private key has been normally generated to form a key pair with the public key under the condition that the private key corresponding to the public key is generated; and

e2) issuing the certificate if the private key has been normally generated.

4. The method of claim 1, wherein the database storage unit includes:

a user information database for storing the reference number for the certificate issuance and user information under
5 the condition that the user is registered as a member in the authentication system; and

a biometric information database for storing the biometric information of the user registered as the member, the user information and the biometric information being
10 registered and stored in such a way as to be matched with each other.

5. The method of claim 1, wherein the user system includes a biometric information input unit for inputting the biometric
15 information of the user.

6. The method of claim 1, wherein the biometric information is information about a user's unique fingerprint.

20 7. The method of claim 1, wherein the biometric information is information about a user's unique iris.

8. The method of claim 1, wherein the biometric information

is information about a user's unique face feature vector.

10082110.022602